ELSEVIER
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Combinatorial Theory, Series A 108 (2004) 247–259
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

Cyclic codes with few weights and Niho exponents

Pascale Charpin

INRIA, Domaine de Voluceau, BP 105-78153 Rocquencourt, Le Chesnay Cedex, France

Received 7 August 2003

Communicated by Vera Pless
Available online 19 August 2004

Abstract

This paper studies the values of the sums

$$S_k(a) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k + ax)}, \quad a \in \mathbf{F}_{2^m},$$

where Tr is the trace function on $\mathbf{F}_{2^m}$, $m = 2t$ and $gcd(2^m - 1, k) = 1$. We mainly prove that when $k \equiv 2^j \pmod{2^t - 1}$, for some j, then $S_k(a)$ takes at least four values when a runs through $\mathbf{F}_{2^m}$. This result, and other derived properties, can be viewed in the study of weights of some cyclic codes and of crosscorrelation function of m-sequences.

Keywords: Finite field; Cyclic code; Maximum-length sequence; Niho exponent; Crosscorrelation; Boolean function; Nonlinearity; Balanced codeword

1. Introduction

The computation of the trace function applied to polynomials of $\mathbf{F}_{2^m}[x]$, where $\mathbf{F}_{2^m}$ is the finite field of order 2^m, is related with several general problems, especially in coding theory. This problem is strongly connected with the study of the weights of some cyclic codes, but also with the study of the spectrum of some sequences and of some Boolean functions.

E-mail address: Pascale.Charpin@inria.fr

0097-3165/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2004.07.001

We treat binary cyclic codes which have two nonzeros only. Such a code is here of length $n = 2^m - 1$, $m = 2t$, and of dimension $2m$. To study its weights is actually to compute the sums

$$S_k(a) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k + ax)}, a \in \mathbf{F}_{2^m},$$

where k and n are coprime and Tr is the trace function on $\mathbf{F}_{2^m}$. These sums can be seen as the Fourier-transforms of the Boolean function $x \mapsto Tr(x^k)$. Moreover, the function $a \mapsto S_k(a)$ provides the crosscorrelation function of one m-sequence of length n with its decimation by k. Our work is based on [9]; in this paper, Helleseth proved that *$S_a(k)$, a in $\mathbf{F}_{2^m}^*$, takes on at least three values, if and only if k is not a power of 2*. At the end of [9], the author stated two conjectures on m-sequences which can be replaced in these two general problems:

$\mathscr{P}_1$: Determine the values of m and k such that $S_k(a)$ takes on at least four values when a runs through $\mathbf{F}_{2^m}^*$.

$\mathscr{P}_2$: Fixing m, determine the integers k such that $S_k(a) = 0$ for at least one nonzero a. In this case, which elements a provide $S_k(a) = 0$?

In the next section, we briefly explain the context and the connections between several objects (codes, sequences and Boolean functions). We state or recall some useful properties.

Our results are presented in Section 3. We treat a specific class of values of k, the so-called *Niho exponents*; these exponents are such that k modulo $2^t - 1$ is a power of 2. We also assume that $gcd(k, n) = 1$ and that k is not a power of 2. We will denote by $\mathscr{N}_m$ this set of Niho exponents with respect to the finite field $\mathbf{F}_{2^m}$, $m = 2t$.

Our main result is related with the problem $\mathscr{P}_1$, since we prove that for $k \in \mathscr{N}_m$ the sum $S_k(a)$ takes on at least four values (Theorem 2) when a runs through $\mathbf{F}_{2^m}^*$. We first establish that the values 0 and -2^t always appear for some nonzero a (Corollary 1).

Several derived results are presented later, in Section 3.1. We propose lower bounds on the maximal value of $S_k(a)$, depending on the values k and m. These bounds can be reached (see Example 1). We contribute to Problem $\mathscr{P}_2$, by characterizing those $k \in \mathscr{N}_m$ such that $S_k(1) = 0$ (Proposition 3). We deduce that $S_k(1) = 0$ is impossible when $m \equiv 2$ modulo 4.

To conclude, we recall some conjectures and open problems. We emphasize that the conjectures due to Helleseth [9] are here strengthened, but remain open problems.

Main notation:

- $n = 2^m - 1$; $m = 2t$;
- $\mathbf{F}_{2^m}$ is the finite field of order 2^m; $\mathbf{F}_{2^m}^* = \mathbf{F}_{2^m} \setminus \{0\}$;
- α is a primitive root of $\mathbf{F}_{2^m}$;
- $\mathscr{G}$ is the cyclic subgroup of order $2^t + 1$: $\mathscr{G} = \langle \alpha^{2^t - 1} \rangle$;
- $wt(u)$ is the Hamming weight of the vector u;
- Tr is the trace-function on $\mathbf{F}_{2^m}$;
- T_s^r the trace-function from $\mathbf{F}_{2^r}$ to $\mathbf{F}_{2^s}$;
- $gcd(A, B)$ is the greatest common divisor of A and B;
- $\mathscr{N}_m$ is the set of integers k satisfying (8) and (9).

2. Preliminaries

We assume that the reader is familiar with finite algebraic objects which are presented here. Our main reference for algebraic coding theory is [14]. For cyclic codes with two zeros and for sequences, more details can be found in [5,10].

2.1. Context

In this paper, our ambient field is $\mathbf{F}_{2^m}$, the finite field of order 2^m with $m = 2t$. We denote by α a primitive root of $\mathbf{F}_{2^m}$. The trace-function from $\mathbf{F}_{2^m}$ to $\mathbf{F}_2$ is denoted by Tr.

We are interested in the weight polynomials of some binary cyclic codes of length $n = 2^m - 1$ which have *two nonzeros only*, α^{-1} and α^{-k}, where $3 \leqslant k \leqslant 2^m - 2$ and $gcd(k, n) = 1$. Such a code is denoted by C_k. Any codeword of C_k, say $\mathbf{c}(y) = \sum_{i=0}^{n-1} c_i y^i$, can be simply expressed by its so-called ms-*polynomial*:

$$Q_{\mathbf{c}}(x) = Tr(ux^k + vx),\ u = \mathbf{c}(\alpha^{-k}) \text{ and } v = \mathbf{c}(\alpha^{-1}), \tag{1}$$

providing, $Q_{\mathbf{c}}(\alpha^i) = c_i$ for all i [1]. For any pair (u, v) of elements of $\mathbf{F}_{2^m}$ the corresponding codeword of length n is the ordered sequence of binary symbols:

$$Q_{\mathbf{c}}(\alpha^0),\ Q_{\mathbf{c}}(\alpha^1), \ldots,\ Q_{\mathbf{c}}(\alpha^{n-1}). \tag{2}$$

We denote by $wt(\mathbf{c})$ the Hamming weight of $\mathbf{c}$, the integer sum of the $Q_{\mathbf{c}}(\alpha^i)$. A codeword is said to be *balanced* when $wt(\mathbf{c}) = 2^{m-1}$.

Since k and n are coprime, to study the weight polynomial of C_k is to study the weights corresponding to the pairs $(1, v)$, $v \in \mathbf{F}_{2^m}$. In other words, *to know the values* $\sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k + ax)}$, $a \in \mathbf{F}_{2^m}$, *and the number of times they occur, is exactly to know the weight polynomial of the code* C_k.

The *Simplex code* is the $[n, m]$ binary cyclic code composed of codewords $\mathbf{c}$, as previously defined (see (2)), with ms-polynomials

$$Q_{\mathbf{c}}(x) = Tr(ax), a \in \mathbf{F}_{2^m}.$$

A *maximum-length sequence*, called m-sequence, is simply a codeword of the *Simplex* code. More generally, choosing any primitive root of $\mathbf{F}_{2^m}$, say α^k, m-sequences are produced by $Tr(ux^k)$, for some u.

The distance between an m-sequence $\mathbf{s}$ and all cyclic shifts of another m-sequence $\mathbf{s}'$ is computed with the *crosscorrelation function*. When the sequence $\mathbf{s}'$ is a *decimation* of $\mathbf{s}$ by k, the crosscorrelation function between $\mathbf{s}$ and $\mathbf{s}'$ becomes:

$$\theta_k(\lambda) = \sum_{x \in \mathbf{F}_{2^m}^*} (-1)^{Tr(x^k + \alpha^\lambda x)},\ 0 \leqslant \lambda \leqslant n - 1.$$

To compute the values of θ_k is to compute the crosscorrelation spectrum of $\mathbf{s}$ and $\mathbf{s}'$. Note that $\theta_k(\lambda) = S_k(\alpha^\lambda) - 1$.

[1] This is the Fourier-transform of the codeword $\mathbf{c}(y)$, which is usually called its Mattson–Solomon polynomial in algebraic coding theory.

In this paper, we need basic tools for computing the Fourier-spectrum of Boolean functions. Our Boolean functions are of the form $f(x) = Tr(P(x))$, $x \in \mathbf{F}_{2^m}$ and P is some polynomial on $\mathbf{F}_{2^m}$. Let us define the linear Boolean functions as follows:

$$\varphi_a : x \mapsto Tr(ax), a \in \mathbf{F}_{2^m}^*.$$

The *Fourier transform* of f in some point $a \in \mathbf{F}_{2^m}$ is denoted $\mathscr{F}_a(f)$ and calculated as follows:

$$\mathscr{F}_a(f) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{f(x)+\varphi_a(x)}.$$

The values of these coefficients form the *Fourier-spectrum* of f, generally denoted $\mathscr{S}_f$. Recall the well-known Parseval's relation

$$\sum_{a \in \mathbf{F}_{2^m}} \mathscr{F}_a^2(f) = 2^{2m} \tag{3}$$

and also this inverse formula

$$\sum_{a \in \mathbf{F}_{2^m}} \mathscr{F}_a(f) = 2^m (-1)^{f(0)}. \tag{4}$$

It is easy to see that not all values in $\mathscr{S}_f$ have the same sign. This is because

$$\left(\sum_{a \in \mathbf{F}_{2^m}} \mathscr{F}_a(f) \right)^2 = \sum_{a \in \mathbf{F}_{2^m}} \mathscr{F}_a^2(f)$$

which implies that it is impossible to have $\mathscr{F}_a(f) \geqslant 0$ for all a as well as $\mathscr{F}_a(f) \leqslant 0$ for all a, unless f is affine.

Lemma 1. *Let f be any non-affine Boolean function. Then there are at least two values in its Fourier-spectrum $\mathscr{S}_f$, say λ and μ, such that $\lambda > 0$ and $\mu < 0$.*

Let $g = f + \varphi_a$, for some a. Considering the sequence of values

$$\mathbf{v} = g(0), g(\alpha^0), \ldots, g(\alpha^{n-1})$$

as a codeword of length 2^m, the weight of $\mathbf{v}$ is related to $\mathscr{F}_a(f)$ via

$$wt(\mathbf{v}) = 2^{n-1} - \frac{\mathscr{F}_a(f)}{2}. \tag{5}$$

The *nonlinearity* of f is the minimal value of $wt(\mathbf{v})$ when a runs through $\mathbf{F}_{2^m}$, i.e. the maximal absolute value of $\mathscr{F}_a(f)$. The function g is said to be *balanced* if and only if $\mathbf{v}$ is a balanced codeword. That is $\mathscr{F}_a(f) = 0$.

To compute the values $\mathscr{F}_a(f)$, when $f(x) = Tr(x^k)$, is exactly to compute $S_k(a)$, $a \in \mathbf{F}_{2^m}$. We will be interested later in the maximal absolute value of $S_k(a)$, which we denote by $\mathscr{L}(k)$ (see Proposition 2). This is exactly the so-called *nonlinearity* of the function $x \mapsto Tr(x^k)$.

2.2. Basic properties

The next lemma is an instance of a classical formula, but we prove it for clarity. Note that the duality is defined here with respect to the inner product $(x, y) \mapsto Tr(xy)$.

Lemma 2. *Let f be any Boolean function on $\mathbf{F}_{2^m}$, where $m = 2t$. Then*

$$\sum_{a\in\mathbf{F}_{2^t}} \mathscr{F}_a(f) = 2^t \sum_{x\in\mathbf{F}_{2^t}} (-1)^{f(x)}$$

Proof. Simply by writing

$$\sum_{a\in\mathbf{F}_{2^t}} \mathscr{F}_a(f) = \sum_{a\in\mathbf{F}_{2^t}} \sum_{x\in\mathbf{F}_{2^m}} (-1)^{f(x)+Tr(ax)} = \sum_{x\in\mathbf{F}_{2^m}} (-1)^{f(x)} \left(\sum_{a\in\mathbf{F}_{2^t}} (-1)^{Tr(ax)} \right)$$
$$= 2^t \sum_{x\in\mathbf{F}_{2^t}} (-1)^{f(x)}.$$

Since $Tr(xy) = 0$ for any $x, y \in \mathbf{F}_{2^t}$, then $\mathbf{F}_{2^t}^{\perp} = \mathbf{F}_{2^t}$. Thus $\sum_{a\in\mathbf{F}_{2^t}} (-1)^{Tr(ax)}$ is equal to 0 unless $x \in \mathbf{F}_{2^t}$; when $x \in \mathbf{F}_{2^t}$, this sum is equal to 2^t. □

The next result is connected with Problem $\mathscr{P}_2$ of Section 1, concerning the determination of balanced codewords.

Lemma 3. *Let $m \geqslant 4$ and set $t = \lceil m/2 \rceil$. Let f be a Boolean function of m variables whose Fourier-spectrum is as follows*:

$$\mathscr{S}_f = \{\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_\mu\}, \mu \geqslant 2, \lambda_0 = 0, 0 < |\lambda_i| < 2^m \text{ for } i \neq 0.$$

We denote by N_i the number of times λ_i occurs

$$N_i = \text{card}\{b | \mathscr{F}_b(f) = \lambda_i\}, \quad 0 \leqslant i \leqslant \mu.$$

If, for all i, $\lambda_i \equiv 0 \pmod{2^t}$ then $N_0 > 1$.

Proof. This result is directly deduced from Parseval's relation (see (3)). From hypothesis we can set $\lambda_i = 2^t a_i$ where $|a_i| > 0$ for any $i \neq 0$. Thus

$$\sum_{i=1}^{\mu} N_i \lambda_i^2 = 2^{2m} = 2^{2t} \sum_{i=1}^{\mu} N_i a_i^2. \tag{6}$$

Let us suppose that $\sum_{i=1}^{\mu} N_i = 2^m - 1$. We have

1. If m is odd then $2t = m + 1$ implying $\sum_{i=1}^{\mu} N_i a_i^2 = 2^{m-1}$.
2. If m is even then $2t = m$ and $\sum_{i=1}^{\mu} N_i a_i^2 = 2^m$.

These two cases lead each to some contradiction. For case 1, it is because we get $\sum_{i=1}^{\mu} N_i \leqslant 2^{m-1}$. When m is even, we get a sum of $2^m - 1$ squares, each a_i^2 repeated N_i times, which is equal to 2^m. This would imply that $a_j^2 = 2$ and $(N_j = 1)$ for one j. □

3. Main results

Let $n = 2^m - 1$ where $m = 2t$. Let us denote by $\mathscr{G}$ the cyclic subgroup of $\mathbf{F}_{2^m}^*$ of order $2^t + 1$. Let k be an integer in the range $[1, n-1]$. From now on, we consider the sums

$$S_k(a) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k + ax)}, a \in \mathbf{F}_{2^m}, \tag{7}$$

with the hypothesis

$$gcd(k, n) = 1, k \notin \{1, 2, 2^2, \ldots, 2^{m-1}\} \tag{8}$$

and

$$k \equiv 2^j \pmod{2^t - 1} \text{ for some } j, 0 \leqslant j \leqslant t - 1. \tag{9}$$

Such exponents k are currently called the *Niho exponents* since they were first studied by Niho in his thesis [13]. We denote by $\mathscr{N}_m$ the set of Niho exponents defined by (8) and (9). Without loss of generality, we can assume that k is in the so-called *normalized form*, that is

$$k = (2^t - 1)s + 1, 0 < s < 2^t - 1. \tag{10}$$

Note that $k \equiv -2s + 1$ modulo $2^t + 1$. From now on, we use this notation

$$\tau \equiv k \pmod{2^t + 1}, 0 < \tau \leqslant 2^t. \tag{11}$$

The next result appeared first in [13] and a proof can be found in [7]. To be clear with our terminology, we indicate the proof. We denote by T_s^r, the trace-function from $\mathbf{F}_{2^r}$ to $\mathbf{F}_{2^s}$, s dividing r.

Theorem 1. *Let $k \in \mathscr{N}_m$; k and τ are defined by (10) and (11). Then $S_k(a) = (N(a) - 1)2^t$, where $N(a)$ is the number of $y \in \mathscr{G}$ such that*

$$y^{2\tau} + ay^{\tau+1} + a^{2^t} y^{\tau-1} + 1 = 0. \tag{12}$$

Proof (*Sketch*). Let α be a primitive root of $\mathbf{F}_{2^m}$. Since $2^t - 1$ and $2^t + 1$ are coprime, any element $z \in \mathbf{F}_{2^m}^*$ can be expressed as follows:

$$z = \alpha^{e(2^t+1)+\ell(2^t-1)}, 0 \leqslant e \leqslant 2^t - 2, 0 \leqslant \ell \leqslant 2^t.$$

Then we have for any fixed $a \neq 0$ and for all $z \in \mathbf{F}_{2^m}^*$:

$$\begin{aligned} Tr(z^k + az) &= T_1^t T_t^m \left((\alpha^{e(2^t+1)+\ell(2^t-1)})^k + a\alpha^{e(2^t+1)+\ell(2^t-1)} \right), \\ &= T_1^t \left(T_t^m (\alpha^{\tau\ell(2^t-1)} + a\alpha^{\ell(2^t-1)})\alpha^{e(2^t+1)} \right). \end{aligned}$$

Hence

$$\begin{aligned} S_k(a) &= 1 + \sum_{y \in \mathscr{G}} \sum_{x \in \mathbf{F}_{2^t}^*} (-1)^{T_1^t (T_t^m (y^\tau + ay)x)} \\ &= -2^t + \sum_{y \in \mathscr{G}} \sum_{x \in \mathbf{F}_{2^t}} (-1)^{T_1^t (T_t^m (y^\tau + ay)x)}. \end{aligned} \tag{13}$$

Thus $S_k(a) = (N(a) - 1)2^t$, where $N(a)$ is the number of those $y \in \mathscr{G}$ which satisfy $y^\tau + ay \in \mathbf{F}_{2^t}$, that is

$$y^\tau + ay + y^{-\tau} + a^{2^t} y^{-1} = 0.$$

The proof is completed by multiplying the equation above by y^τ. □

Therefore, according to the previous theorem, we can apply Lemmas 1 and 3 to the Boolean non-affine function defined by $f(x) = Tr(x^k)$. Indeed, there is only one suitable negative value of $S_k(a)$ and the nonzero Fourier-coefficients of such f are divisible by 2^t.

Corollary 1. *Let $S_k(a)$ be defined by (7) with $k \in \mathscr{N}_m$. Then there is at least one $a \neq 0$ and one $b \neq 0$ such that, respectively,*

$$S_k(a) = -2^t \text{ and } S_k(b) = 0.$$

Remark 1. The integer τ, defined by (10), satisfies

$$gcd(\tau, 2^t + 1) = 1 \quad \text{and} \quad \tau \neq 2^t.$$

Indeed, if there is $e > 1$ which divides $gcd(\tau, 2^t + 1)$ then e divides k, a contradiction since $gcd(k, 2^t + 1) = 1$. On the other hand, if $\tau = 2^t$ then $2^t \equiv k$ (modulo $2^t + 1$). Since $k = (2^t - 1)s + 1$, we get $2^t \equiv -2s + 1$ which implies $2s - 2 \equiv 0$. This is impossible unless $k = 2^t$.

Remark 2. The exact divisibility of the codes C_k, where $k \in \mathscr{N}_m$, was also proved in [2, Theorem7.5] by using McEliece's theorem. The weight polynomials of these codes, for $m = 6, 8$ and 10, can be found in [2, p.130].

Now we are going to prove our main result.

Theorem 2. *Let $m = 2t$ and let $k \in \mathscr{N}_m$. Then the sum*

$$S_k(a) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k + ax)},$$

takes at least four values when a runs through $\mathbf{F}_{2^m}^*$.

Proof. We assume that k is in its normalized form, as in (10); τ is defined by (11). Let us denote by $\mathscr{V}$ the set of values $S_k(a)$, $a \in \mathbf{F}_{2^m}^*$. We know that the cardinality of $\mathscr{V}$ is at least 3 [9]. We assume that it is exactly 3. Then, from Theorem 1 and Corollary 1, we actually suppose that $\mathscr{V} = \{0, -2^t, \gamma\}$, where $\gamma = 2^t \Delta$, with $\Delta > 0$.

First, we consider (12) for any nonzero a in the subfield $\mathbf{F}_{2^t}$. We get

$$y^{2\tau} + a(y^{\tau+1} + y^{\tau-1}) + 1 = 0. \tag{14}$$

Clearly $y = 1$ is a solution, for any a. Also, $y \in \mathscr{G}$ is a solution if and only if y^{2^t} is a solution. Thus, for any $a \in \mathbf{F}_{2^t}$, the number $N(a)$ of solutions of the above equation is such that $N(a) = 1 + 2\ell$ for some ℓ. According to Theorem 1, we get $\gamma = \ell 2^{t+1}$. Now we apply

Lemma 2 to the Boolean function defined by $f(x) = Tr(x^k)$. With $S_k(a) = \mathscr{F}_a(f)$, we get

$$\sum_{a\in\mathbf{F}_{2^t}} S_k(a) = 2^t \sum_{x\in\mathbf{F}_{2^t}} (-1)^{Tr(x^k)} = 2^m, \tag{15}$$

because $f(x) = 0$ for all $x \in \mathbf{F}_{2^t}$. But in the sum above (on the left), each nonzero term is divisible by 2^{t+1} and then, by hypothesis, must be equal to γ. Thus $2^m = L\gamma$, for some L, providing $\gamma = 2^\rho$ with $\rho \geqslant t+1$.

In order to prove that the cardinality of $\mathscr{V}$ cannot be three, it remains to prove that there is some $a \in \mathbf{F}_{2^m}^*$ such that $S_k(a)$ is not in $\{0, -2^t, 2^\rho\}$. In other words, there is some $a \in \mathbf{F}_{2^m}^*$ such that:

$$N(a) > 1 \text{ and } (N(a)-1)2^t \neq 2^\rho (\text{where } \rho \geqslant t+1). \tag{16}$$

Consider now $S_k(a)$ with $a \in \mathscr{G} \setminus \{1\}$. As $aa^{2^t} = 1$, (12) becomes

$$y^{2\tau} + ay^{\tau+1} + a^{2^t} y^{\tau-1} + aa^{2^t} = (y^{\tau+1} + a^{2^t})(y^{\tau-1} + a) = 0.$$

Thus $N(a)$ is equal to the number of solutions $y \in \mathscr{G}$ satisfying

$$y^{\tau+1} + a^{2^t} = 0 \tag{17}$$

or

$$y^{\tau-1} + a = 0. \tag{18}$$

Note that y cannot be a solution of both equations above. Indeed, this would imply $y^{2\tau} = 1$, which is impossible since 2τ and $2^t + 1$ are coprime. Also, it is impossible to have $\tau + 1 = 2^t + 1$ (see Remark 1).

We set $e = gcd(\tau + 1, 2^t + 1)$ and $e' = gcd(\tau - 1, 2^t + 1)$. Let β be a generator of $\mathscr{G}$. Then we have:

1. If $e = e' = 1$ then (17) and (18) each have one and only one solution providing $N(a) = 2$. Thus (16) is satisfied for any a.

2. Assume that $e > 1$ and $e' = 1$. There is only one solution for (18), for any a. Choosing $a = \beta^{-(\tau+1)}$ (for instance) then the solutions of (17) are

$$\{\beta, \beta^{1+v}, \ldots, \beta^{1+(e-1)v}\}, \text{ where } v = (2^t+1)/e.$$

We get $N(a) = e + 1$ which satisfies (16), since $N(a) - 1$ is odd. Note that the situation is similar when $e = 1$ and $e' > 1$, by choosing $a = \beta^{\tau-1}$.

3. Now suppose that $e > 1$ and $e' > 1$. Note that $gcd(e, e') = 1$, since $gcd(\tau - 1, \tau + 1) \leqslant 2$; in particular $e \neq e'$.

By taking $a = \beta^{-(\tau+1)}$, then (17) has e solutions. Moreover there is no solution of (18) for this a, because this would imply that e' divides $\tau + 1$ too. Hence $N(a) = e$. Similarly, choosing $a' = \beta^{\tau-1}$ we obtain $N(a') = e'$. Thus, we get two different values, $N(a) \geqslant 3$ and $N(a') \geqslant 3$ corresponding to two distinct elements of $\mathscr{G}$. At least one of these values satisfies (16), completing the proof. □

Remark 3. It is important to complete Theorem 2, by noticing that $S_k(a)$ takes exactly four values for $k = 2^{t+1} - 1$(see Example 1 later). This case was fully solved by Niho in his thesis where these values and the number of times they occur were given, even when $gcd(k, n) \neq 1$ [13]. This result was generalized to odd characteristics by Helleseth [9].

3.1. Derived results

This section is an extension of the previous one, where we focused on the number of values $S_k(a)$. Notation is as in the previous section. Notably, $k \in \mathcal{N}_m$ and τ are defined by (8)–(11). The proof of Theorem 2 leads us to several partial results concerning $\mathcal{V}$, the set of the values of $S_k(a)$. We have from Theorem 1, Corollary 1 and Theorem 2:

$$\mathcal{V} = \{0, -2^t, \delta_1 2^t, ..., \delta_i 2^t\}, 2 \leqslant i, 0 < \delta_j < \delta_{j+1},$$

where $\delta_j = N(a) - 1$ for some a. It appeared that $S_k(a) \equiv 0$ modulo 2^{t+1} for all $a \in \mathbf{F}_{2^t}$ (see (14)). Moreover some such $S_k(a)$ are not zero. Indeed we can deduce from (15):

$$2 \leqslant \text{card}\{a \in \mathbf{F}_{2^t} | S_k(a) \neq 0\} \leqslant 2^{t-1}.$$

Therefore, the maximal value of $S_k(a)$, which we denote by $\mathcal{L}(k)$, is greater than or equal to 2^{t+1}. If $\mathcal{L}(k) = 2^{t+1}$ then $\mathcal{V}$, which must have at least four elements, contains 0, $\pm 2^t$ and 2^{t+1} only. Moreover, in this case, any nonzero $S_k(a)$, with $a \in \mathbf{F}_{2^t}$, is equal to 2^{t+1}. More generally, assume that $\mathcal{V}$ has four elements only, three of them being 0, -2^t and $\delta 2^t$ for some odd δ. Then all nonzero $S_k(a)$, with $a \in \mathbf{F}_{2^t}$, are equal to the fourth element of $\mathcal{V}$. Moreover, as before by using (15), we claim that this fourth weight is 2^ρ with $\rho \geqslant t + 1$. In the cases **1.** and **2.** of the proof of Theorem 2, we obtained odd values for $N(a) - 1$ (for some $a \in \mathcal{G}$). Thus we proved the following property.

Proposition 1. *Assume that the sum $S_k(a)$, $k \in \mathcal{N}_m$, takes four values only, when a runs through $\mathbf{F}_{2^m}$. Recall that*

$$e = gcd(\tau + 1, 2^t + 1) \text{ and } e' = gcd(\tau - 1, 2^t + 1).$$

If $e = 1$ or $e' = 1$ then $S_k(a) = 2^\rho$ with $\rho \geqslant t + 1$, for all $a \in \mathbf{F}_{2^t}$ such that $S_k(a) \neq 0$. Moreover we have:

- *if $e = e' = 1$ then $\mathcal{V} = \{0, \pm 2^t, 2^\rho\}$;*
- *if $e = 1$ and $e' > 1$ then $\mathcal{V} = \{0, -2^t, e'2^t, 2^\rho\}$;*
- *if $e > 1$ and $e' = 1$ then $\mathcal{V} = \{0, -2^t, e2^t, 2^\rho\}$.*

Now look at other consequences of our results on $S_k(a)$ for $a \in \mathcal{G} \setminus \{1\}$. In the case 1, we show that $S_k(a) = 2^t$ for any such a. With the hypothesis of 2, we characterize some a such that $S_k(a) = e2^t$ with $e \geqslant 3$. With the hypothesis of 3, we obtain some a such that $S_k(a) = (e - 1)2^t$ and some a' such that $S_k(a') = (e' - 1)2^t$ with $e \geqslant 3$, $e' \geqslant 3$ and $e \neq e'$. Hence $\mathcal{L}(k) = 2^{t+1}$ is possible in the case 1 only. In any case, we get a lower bound on $\mathcal{L}(k)$.

When t is odd then 3 divides 2^t+1, which implies that 3 is not a divisor of τ (see Remark 1). Then either $\tau-1$ or $\tau+1$ (and not both) are divisible by 3. Thus, when t is odd then the case 1 is impossible and we are sure that $\mathscr{L}(k) > 2^{t+1}$. We summarize these results in the next proposition. Recall that $k \in \mathscr{N}_m$, $m = 2t$.

Proposition 2. (i) *For all* $a \in \mathbf{F}_{2^t}$, $S_k(a) \equiv 0$ *modulo* 2^{t+1}; *moreover at least* 2 (*and at most* 2^{t-1}) *such a provide* $S_k(a) \neq 0$. *Therefore*

$$\mathscr{L}(k) \geqslant 2^{t+1}, \text{ where } \mathscr{L}(k) = \max_{a \in \mathbf{F}_{2^m}} |S_k(a)|.$$

(ii) *If* $\mathscr{L}(k) = 2^{t+1}$ *then* $e = e' = 1$ *and* $S_k(a)$ *takes exactly four values,* $\{0, \pm 2^t, 2^{t+1}\}$; *the value* 2^{t+1} *occurs at least* 2^{t-1} *times*.
(iii) *If* $e = e' = 1$ *then* $S_k(a) = 2^t$ *for all* $a \in \mathscr{G} \setminus \{1\}$.
(iv) *If only one element of the pair* (e, e') *is equal to* 1, *say* $e' = 1$, *then* $\mathscr{L}(k) \geqslant e2^t$ *and there is some* a *such that* $S_k(a) = e2^t$.
(v) *If* $e > 1$ *and* $e' > 1$ *then* $S_k(a)$ *takes the value* $(e-1)2^t$ *for some* a *and the value* $(e'-1)2^t$ *for another* a; *therefore*:

$$\mathscr{L}(k) \geqslant E2^t, \text{ where } E = \max\{e-1, e'-1\}.$$

(vi) If $m \equiv 2 \pmod 4$ *then* $\mathscr{L}(k) > 2^{t+1}$.

Example 1. Lower bounds on $\mathscr{L}(k)$ are proposed in the previous proposition; they are reached for some values of k (and m). We illustrate this by two well-known examples. The first one is given in Remark 3, that is $k = 2^{t+1}-1$. We have to solve (12) with $\tau = 3$, $\tau - 1 = 2$ and $\tau + 1 = 4$, implying $e = e' = 1$. In this case $\mathscr{L}(k) = 2^{t+1}$.

When $k = 2^t + 3$, we consider its normalized form:

$$k = (2^{t-2}+1)(2^t-1)+1, \tau \equiv 2^{t-2}(2^t+3) \equiv 2^{t-1} \pmod{2^t+1}.$$

It is known that $\mathscr{L}(k) = 3 \times 2^t$ (see [9, Theorem 4.8]). According to the previous proposition we are sure that at least one element of the pair (e, e') is equal to 1. If t is odd then 3 divides 2^t+1 and $\tau - 1$; thus we must have $e = 1$ and $e' = 3$. For instance for $m = 10$ and $k = 35$ we get $\tau = 16$, $2^t + 1 = 33$, $\tau - 1 = 15$ and $\tau + 1 = 17$. But take for instance $m = 8$ and $k = 19$; here we have $e = e' = 1$ since $2^t + 1$ is prime.

We can also derive some results related with the problem $\mathscr{P}_2$, to characterize some set of balanced codewords. In accordance with Theorem 1, $S_k(a) = 0$ if and only if the equation

$$y^{2\tau} + ay^{\tau+1} + a^{2^t} y^{\tau-1} + 1 = 0,$$

has one and only one solution $y \in \mathscr{G}$.

Proposition 3. *For any* $k \in \mathscr{N}_m$, *we have*:

$$S_k(1) = \sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k+x)} = 0 \Longleftrightarrow e = e' = 1.$$

Moreover, in this case,

$$gcd(y^{2\tau} + y^{\tau+1} + y^{\tau-1} + 1, y^{2^t+1} + 1) = y + 1.$$

Notably, if t is odd then $S_k(1) \neq 0$.

In other words, the binary codeword $\mathbf{c}$ *of length* $2^{2t} - 1$ *with* ms*-polynomial* $Q_{\mathbf{c}}(x) = Tr(x^k + x)$ *is balanced if and only if t, k and* τ *are such that* $e = e' = 1$.

Proof. It is simply deduced from

$$y^{2\tau} + y^{\tau+1} + y^{\tau-1} + 1 = (y^{\tau+1} + 1)(y^{\tau-1} + 1).$$

The polynomial above has one and only one root in $\mathscr{G}$ (which is $y = 1$) if and only if $gcd(\tau - 1, 2^t + 1) = gcd(\tau + 1, 2^t + 1) = 1$.

As we previously noticed, this last condition is impossible when t is odd. □

Example 2. For $m = 8$ and 16 then $2^t + 1$ is equal, respectively to 17 and 257, which are prime numbers. Thus, in these cases, $S_k(1) = 0$ for any $k \in \mathscr{N}_m$. On the contrary, if $m = 4s$ with s odd, there are different situations. Take for instance $m = 12$; so $t = 6$, $2^t - 1 = 63$ and $2^t + 1 = 65$:

- If $k = 67 = 64 + 3$ then $\tau = 32$ (see Example 1). Since $gcd(65, 31)$ and $gcd(65, 33)$ are equal to 1 then $S_k(1) = 0$.
- If $k = 5 \times 63 + 1$ then $\tau = 56$. Since $gcd(65, 55) = 5$ and $gcd(65, 57) = 1$ then $S_k(1) \neq 0$. Moreover $\mathscr{L}(k) \geqslant 5 \times 2^6$.

When $\tau = 3$, Eq. (12) becomes

$$y^6 + ay^4 + a^{2^t} y^2 + 1 = 0,$$

which has at most three solutions. Therefore, we deduce from Theorem 1 that $\mathscr{L}(k) \leqslant 2^{t+1}$, implying that the set of values of $S_k(a)$ is exactly $\{0, \pm 2^t, 2^{t+1}\}$. (see, for instance, Example 1). This suggests a method for finding $\mathscr{L}(k)$ for some values of k.

Research problem: Characterize an infinite class of Niho exponents k satisfying:

1. on the one hand, Proposition 2 provides a lower bound for $\mathscr{L}(k)$, say $b2^t$, using $gcd(\tau \pm 1, 2^t + 1)$.
2. on the other hand, τ is such that the equation (12) cannot have more than $b + 1$ solutions.

4. Conclusion

In this paper, we studied the Boolean functions on $\mathbf{F}_{2^m}$, $m = 2t$, of the form $f : x \mapsto Tr(x^k)$ where $k \in \mathscr{N}_m$, i.e., $gcd(2^m - 1, k) = 1$ and k modulo $2^t - 1$ is a power of 2. We noticed that these functions can be seen as a concatenation of linear functions on $\mathbf{F}_{2^t}$. We notably gave an upper bound on their nonlinearity. To find the exact nonlinearity remains an open problem.

It is a long-standing problem to find weight enumerators of cyclic codes with two nonzeros. Most recently, these codes were studied in relation with some cryptographic problems. It appeared that, their minimum weight, the number of their weights and their divisibility are of most interest in this context (see [2–4] and their references).

Concerning the number of weights of codes C_k, the most recent result is due to McGuire, who proved that, *for m even and $k \equiv 0 \pmod 3$, C_k cannot have three weights only* [12]. We define here another large class of codes C_k (for $k \in \mathcal{N}_m$) which cannot have three nonzero weights. Moreover we prove that, for these codes, the number of balanced codewords is strictly greater than $2^{t-1}(2^m-1)$. Note that the next well-known conjecture is satisfied when k is a Niho exponent (see Proposition 2).

Conjecture 1. *Let $m = 2t$; let C_k be the $[2^m-1, 2m]$ binary cyclic code with two nonzeros, α^{-1} and α^{-k}. Then the minimum distance of C_k is smaller than or equal to $2^{m-1} - 2^t$.*

Consider two binary m-sequences, any m-sequence and its decimation by k. For even m, we exhibit here a large class of k such that these sequences cannot have a 3-valued crosscorrelation. Our result strengthens the conjecture stated by Helleseth in [9]:

Conjecture 2. *Two binary m-sequences of length $n = 2^m - 1$ cannot have a 3-valued crosscorrelation function when m is a power of two.*

Calderbank et al. [1] proved that these three values (above) cannot be -1, $-1 + A$ and $-1 - A$ (see also [11]). We contribute to the second conjecture of Helleseth [9, Conjecture 5.1] which can be expressed as follows:

Conjecture 3. *For any m and k such that $gcd(2^m-1, k) = 1$, the sum $\sum_{x \in \mathbf{F}_{2^m}} (-1)^{Tr(x^k+ax)}$ is null for at least one nonzero a.*

Recall that when m is even the maximal nonlinearity of balanced Boolean functions is not known; the most recent results can be found in [6].

Acknowledgements

The author would like to thank Gary McGuire. This work is based on many interesting and valuable discussions with him on the weights of cyclic codes and related topics. She wish to thank Hans Dobbertin and Tor Helleseth, for sending her their preprint concerning Niho exponents [8], and for helpful comments which highly improved the manuscript.

References

[1] R. Calderbank, G. McGuire, B. Poonen, M. Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-sequences, IEEE Trans. Inform. Theory 42 (1996) 988–990.

[2] A. Canteaut, P. Charpin, H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences, SIAM J. Discrete Math. 13 (1) (2000) 105–138.

[3] A. Canteaut, P. Charpin, M. Videau, Cryptanalysis of block ciphers and weight divisibility of some binary codes, in: M. Blaum, P.G. Farrell, H. van Tilborg (Eds.), Information, Coding and Mathematics, Academic Publisher, Kluwer, 2002, pp. 75–97.
[4] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes Cryptogr. 15 (1998) 125–156.
[5] P. Charpin, Open Problems on cyclic codes, Handbook of Coding Theory, Part 1: Algebraic Coding, V.S. Pless, W.C. Huffman (Eds.), R.A. Brualdi (assistant ed.), Elsevier, Amsterdam, the Netherlands, 1998 (Chapter 11).
[6] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity, Fast Software Encryption, Lecture Notes in Computer Science, vol. 1008, Springer, Berlin, Germany, 1994, pp. 61–74.
[7] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$. AAECC, Appl. Algebra Eng. Comm. Comput. 9 (1998) 139–152.
[8] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendalh, Niho type cross-correlation functions via Dickson polynomials and Klosterman sums, preprint.
[9] T. Helleseth, Some results about the crosscorrelation function between two maximal linear sequences, Discrete Math. 16 (1976) 209–232.
[10] T. Helleseth, P.V. Kumar, Sequences with low correlation, Handbook of Coding Theory, Part 3: Applications, V.S. Pless, W.C. Huffman (Eds.), R.A. Brualdi (assistant ed.), Elsevier, Amsterdam, the Netherlands, 1998 (Chapter 21).
[11] G. McGuire, On certain 3-weight cyclic codes having symmetric weight and a conjecture of Helleseth, in Proceedings of Sequences and their Applications, SETA 01, Springer, series: Discrete Mathematics and Theoretical Computer Science, Springer, Berlin, 2002, pp. 281–295.
[12] G. McGuire, On three weights in cyclic codes with two zeros, Finite Fields Appl. 10 (2004) 97–104.
[13] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. Thesis, USCEE Rep. 409. University Southern California, 1972.
[14] V.S. Pless, W.C. Huffman, R.A. Brualdi, An introduction to algebraic codes. Handbook of Coding Theory, Part 1: Algebraic Coding, V.S. Pless, W.C. Huffman (Eds.), R.A. Brualdi (assistant ed.), Elsevier, Amsterdam, the Netherlands, 1998 (Chapter 1).